Information Security – Personally Identifiable Information (PII)

Preamble

One of the most widely used terms to describe personal information is PII. PII is "any information about an individual maintained by Yosemite Community College District (YCCD), including:

1. information that can be used to distinguish an individual's identity
2. information that is linked or linkable to an individual, such as medical, educational, financial records.

To *distinguish* an individual is to identify an individual. Some examples of information that could identify an individual include, but are not limited to, name, passport number, social security number, or biometric data (such as a photograph). In contrast, a list containing only grades without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual.

However, Information elements that are not sufficient to identify an individual when considered separately might nevertheless render the individual identifiable when combined (Linked) with additional information. For instance, if the list of grades were to be supplemented with information, such as age, address, and gender, it is probable that this additional information would render the individuals identifiable.

Purpose

To enhance individual privacy for Employees, Faculty and Students of the YCCD through the secure handling of PII and personal identifiers (PIDs);
To increase security and management of Social Security numbers (SSNs) by:

A. inculcating broad awareness of the confidential nature of the SSNs;
B. establishing a consistent policy about the use of SSNs throughout YCCD; and
C. ensuring that access to SSNs for the purpose of conducting District business is granted only to the extent necessary to accomplish a given task or purpose.

Scope

This procedure applies to all members of YCCD, including all full- and part-time employees, faculty, students and their parents or guardians, and other individuals such as contractors, consultants, other agents of the community, alumni, and affiliates that are associated with YCCD or whose work gives them custodial responsibilities for PII.

Information Security – Personally Identifiable Information (PII)

Definitions

Personally Identifiable Information (PII): Examples of PII range from an individual's SSN, name or email address to an individual's financial and medical records or criminal history. Unauthorized access, use, or disclosure of PII can seriously harm both individuals, by contributing to identity theft, blackmail, or embarrassment, and the organization, by reducing public trust in the organization or creating legal liability.

Linked information: information about or related to an individual that is logically associated with other information about the individual.

Linkable information: information about or related to an individual for which there is a possibility of logical association with other information about the individual.

Personal Identifier (PID): unique code assigned to an individual to identify that individual.

Colleague ID: A Colleague ID (PID), is an example of linked information, is a unique code assigned to an individual to identify that individual. Colleague IDs are used primarily, but not exclusively, for the purpose of electronic operations.

YCCD Network ID: A Network ID (PID) is created for every YCCD employee, Network IDs are primarily used to gain access to YCCD networks, servers, workstations, E-mail accounts and software applications.

Least privilege: limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege is giving people the lowest level of user rights that they can have and still do their jobs.

Secure Deletion: Secure deletion of an electronic file is accomplished by overwriting the full file contents with random data multiple times.

privacy incident: as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons, other than authorized users and for an unauthorized purpose, have access or potential access to PII in usable form, whether physical or electronic.

Review of PII

YCCD Information Technology will annually preform a review of PII stored on district servers, the review shall identify the servers and storage devices housing PII data. The review shall also record the quantity and type of PII stored in each location. Each location shall be assigned an impact level according to the type and quantity of PII stored.

Information Security – Personally Identifiable Information (PII)

Impact Levels

1. **Low** - if the loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals.
2. **Moderate** - if the loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.
3. **High** - if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.

   The following factors influence the impact level of PII.
   - Identifiability
   - Quantity of PII
   - Data field sensitivity
   - Context of use
   - Obligation to protect confidentiality
   - Access to and location of PII

Authorization for access

Access to view, modify or delete SSN's and Birthdate's electronically must be requested in writing and accompanied by a written justification of the access needs. Requests must be submitted to YCD Information Systems using the PII Access request Form.

Refer requests for Sensitive PII from members of the media, the public and other outside entities to YCCD Human Resources.

Access

Only access or use Sensitive PII when you have a need to know that information, that is, when your need for the information relates to your official duties.

- Personally owned computers, mobile devices (such as laptops, mobile phones, tablets or removable media) or to systems outside the protection of the district should not be used to access, save, store, or host Sensitive PII.

- When you handle, process, transmit, transport and/or store Sensitive PII, you should limit the potential for unauthorized disclosure. For example, protect against "shoulder surfing" or eavesdropping by being aware of your surroundings when processing or discussing PII.

- When you need to print, copy, or extract Sensitive PII from a larger data set, limit the new data set to include only the specific data elements you need to perform the task at

hand.

- In addition, if you need to create duplicate copies of Sensitive PII to perform a particular task or project, delete or destroy them when they are no longer needed.

Storage

All electronic files that contain PII will reside within a protected YCCD information system location. All physical files containing PII will reside within a locked file cabinet or room when not being actively viewed or modified.

Physically secure Sensitive PII (e.g., in a locked drawer, cabinet, desk, or safe) when not in use or not otherwise under the control of a person with a need to know.

Transmittal

PII shall not be sent through any form of insecure electronic communication E.g. E-mail or instant messaging systems. Security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. Wen transferring PII the data must be encrypted and decryption keys must be transferred separately.

Disposal

When disposing of PII the physical or electronic file should be shredded or securely deleted. Additionally, do not return failed hard drives to vendors for warranty repair or replacement if the device was ever used to store PII. For more information, please refer to YCCD board policy 3310.

Incident Reporting

In the event of a confirmed or suspected Privacy Incident the Assistant Vice Chancellor of Information technology must be informed of Privacy Incident within 1 hour after discovery. E.g. Unauthorized computer access, misplacing a paper report, loss of a laptop, mobile device, or removable media containing PII, accidental email of PII, possible virus, or malware infection or a computer containing PII.

If you suspect a privacy incident has occurred.

- Document or maintain records of information and actions relevant to the incident, as they may be required in the privacy incident handling report.

- Do not forward compromised information (e.g., SSN, full name, birth date, etc.) when reporting an incident. remember that the information is duplicated and further compromised if you forward or reply to it.

Information Security – Personally Identifiable Information (PII)

- Refer to the Information Technology Security Incident Response Administrative procedure